Matrix Coding

Cryptography, to most people, is concerned with keeping communications private. Indeed, the protection of sensitive communications has been the emphasis of cryptography throughout much of its history. Encryption is the transformation of data into some unreadable form. Its purpose is to ensure privacy by keeping the information hidden from anyone for whom it is not intended, even those who can see the encrypted data. Decryption is the reverse of encryption; it is the transformation of encrypted data back into some intelligible form.

Encryption and decryption require the use of some secret information, usually referred to as a key. Depending on the encryption mechanism used, the same key might be used for both encryption and decryption, while for other mechanisms, the keys used for encryption and decryption are different.

Today governments use sophisticated methods of coding and decoding messages. One type of code, which is extremely difficult to break, makes use of a large matrix to encode a message. The receiver of the message decodes it using the inverse of the matrix. This first matrix is called the **encoding matrix** and its inverse is called the **decoding matrix.**

Example Let the message be:

PREPARE TO NEGOTIATE

and the encoding matrix be

$$\begin{bmatrix} -3 & -3 & -4 \\ 0 & 1 & 1 \\ 4 & 3 & 4 \end{bmatrix}$$

We assign a number for each letter of the alphabet. For simplicity, let us associate each letter with its position in the alphabet: A is 1, B is 2, and so on. Also, we assign the number 27 (remember we have only 26 letters in the alphabet, please tell me you know this) to a space between two words. Thus the message becomes:

P	R	E	P	A	R	E	*	T	O	*	N	E	G	O	T	I	A	T	E
16	18	5	16	1	18	5	27	20	15	27	14	5	7	15	20	9	1	20	5

Since we are using a 3 by 3 matrix, we break the enumerated message above into a sequence of 3 by 1 matrices:

$$\begin{bmatrix}16\\18\\5\end{bmatrix}\ \begin{bmatrix}16\\1\\18\end{bmatrix}\ \begin{bmatrix}5\\27\\20\end{bmatrix}\ \begin{bmatrix}15\\27\\14\end{bmatrix}\ \begin{bmatrix}5\\7\\15\end{bmatrix}\ \begin{bmatrix}20\\9\\1\end{bmatrix}\ \begin{bmatrix}20\\5\\27\end{bmatrix}$$

Note that it was necessary to add a space at the end of the message to complete the last matrix. We now encode the message by multiplying each of the above matrices by the encoding matrix. This can be done by writing the above matrices as columns of a matrix and perform the matrix multiplication of that matrix with the encoding matrix as follows:

$$\begin{bmatrix}-3 & -3 & -4\\ 0 & 1 & 1\\ 4 & 3 & 4\end{bmatrix}\begin{bmatrix}16 & 16 & 5 & 15 & 5 & 20 & 20\\ 18 & 1 & 27 & 27 & 7 & 9 & 5\\ 5 & 18 & 20 & 14 & 15 & 1 & 27\end{bmatrix}$$

which gives the matrix

$$\begin{bmatrix}-122 & -123 & -176 & -182 & -96 & -91 & -183\\ 23 & 19 & 47 & 41 & 22 & 10 & 32\\ 138 & 139 & 181 & 197 & 101 & 111 & 203\end{bmatrix}$$

The columns of this matrix give the encoded message. The message is transmitted in the following linear form

-122, -123, -176, -182, -96, -91, -183, 23, 19, 47, 41, 22, 10, 32, 138, 139, 181, 197, 101, 111, 203

To decode the message, the receiver writes this string as a sequence of 3 by 1 column matrices and repeats the technique using the inverse of the encoding matrix. The inverse of this encoding matrix, the decoding matrix, is:

$$\begin{bmatrix}1 & 0 & 1\\ 4 & 4 & 3\\ -4 & -3 & -3\end{bmatrix}$$

(make sure that you compute it yourself). Thus, to decode the message, perform the matrix multiplication

$$\begin{bmatrix}1 & 0 & 1\\ 4 & 4 & 3\\ -4 & -3 & -3\end{bmatrix}\begin{bmatrix}-122 & -123 & -176 & -182 & -96 & -91 & -183\\ 23 & 19 & 47 & 41 & 22 & 10 & 32\\ 138 & 139 & 181 & 197 & 101 & 111 & 203\end{bmatrix}$$

and get the matrix

$$\begin{bmatrix} 16 & 16 & 5 & 15 & 5 & 20 & 20 \\ 18 & 1 & 27 & 27 & 7 & 9 & 5 \\ 5 & 18 & 20 & 14 & 15 & 1 & 27 \end{bmatrix}$$

The columns of this matrix, written in linear form, give the original message:

P	R	E	P	A	R	E	*	T	O	*	N	E	G	O	T	I	A	T	E	*
16	18	5	16	1	18	5	27	20	15	27	14	5	7	15	20	9	1	20	5	27

And the net result, then, is that you should get ready to do some serious negotiating.

Now, in all honesty, nobody would use such a simple code to send important secret messages like WE WILL BOMB HIROSHIMA ON AUGUST SIXTH, D DAY WILL BE TOMORROW, or DISNEY WORLD IS THE PLACE TO BE THIS CHRISTMAS, AND FRANKLY, AT ANY TIME OF ANY YEAR. People sending codes had much more intricate ways of disguising what letters corresponded to what numbers when they used matrices. However, since we are not taking a full class on cryptography, it is not desperately important that we know how to do deeply difficult decoding. But let's look at one simple way that could be used. Instead of having the following as our number to letter set-up:

A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	*
1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27

we could, instead, horizontally shift the letters five positions to the right and get this:

V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	*
1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27

We might shift letters to the left, or reverse them, or assign them numbers that start at 37 and increase by three every time, and so on and so forth. As long as the sender and the receiver know the code that is being used and which number goes with which letter, then all is well in Denmark. If they are not on the same page, then something is rotten in Denmark, and a message will simply look like random letters and mean nothing to the receiver.

EXERCISES

1. Shift the normal 26-letter alphabet five letters to the right in the next problem (it will look like the above row of letters that assigns the letter *V* to 1) to help you solve the following code:

180, 487, 279, 404, 282, 148, 494, 4, -104, -50, -18, -110, -20, -70, 263, 418, 272, 511, 131, 154, 512

where the **decoding** matrix is

$$\begin{bmatrix} -\frac{12}{5} & -\frac{41}{10} & \frac{9}{5} \\ \frac{23}{15} & \frac{79}{30} & -\frac{16}{15} \\ -\frac{8}{5} & -\frac{29}{10} & \frac{6}{5} \end{bmatrix}$$

The actual message is: ____

2. To decode the next message, shift the normal 26-letter alphabet seven letters to the right. Keep number 27 reserved for a space. The decoding matrix is:

$$\begin{bmatrix} \frac{7}{15} & -\frac{13}{15} & \frac{5}{3} & -\frac{2}{3} \\ -\frac{1}{5} & \frac{4}{5} & -2 & 1 \\ \frac{2}{15} & -\frac{8}{15} & \frac{4}{3} & -\frac{1}{3} \\ -\frac{1}{5} & \frac{4}{5} & -1 & 0 \end{bmatrix}$$

The code is: 188, 177, 158, 139, 129, 235, 172, 214, 111, 180, 227, 134, 232, 113, 182, 171, 91, 175, 173, 156, 154, 145, 178, 201, 121, 40, 110, 108, 31, 72, 88, 74, 76, 54, 78, 107, 110, 47, 131, 133, 27, 78, 99, 66, 32, 82, 82

The actual message is: ____

____

3. **Homework problem.** Make up your own message to transmit, encode it, and bring it to class tomorrow. In class, you will give the coded message to a partner as a string of numbers for them to solve. You can use any variation of letter-to-number correspondence you want, as well as any encoding matrix, but be sure to include both for your partner before he or she tries to decode your message.